AMENDMENTS TO THE CLAIMS

Kindly amend claims 1, 9-12, 14-15, 17, and 22 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

an x86-compatible microprocessor, comprising:

an instruction register within a x86-compatible microprocessor having a single, atomic cryptographic instruction disposed therein~~, wherein said single, atomic cryptographic instruction is arranged according to the instruction format for execution on said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and~~ wherein said single, atomic cryptographic instruction prescribes that a user-generated key schedule be employed for execution of ~~said encryption~~an encryption operation, and wherein said encryption operation that is prescribed by said single, atomic cryptographic instruction comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks;

a keygen unit, operatively coupled to said instruction register, configured to direct said x86-compatible microprocessor to load said user-generated key schedule; and

an execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said encryption operation, said execution unit comprising:

a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction; and

an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said encryption operation, wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds.

2. (Cancelled)

3. (Cancelled)

4. (Original) The apparatus as recited in claim 1, wherein said user-generated key schedule is stored in memory.

5. (Original) The apparatus as recited in claim 1, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

6. (Previously Presented) The apparatus as recited in claim 1, wherein said keygen unit is configured to interpret a key generation field within a control word which is referenced by said single, atomic cryptographic instruction.

7. (Cancelled)

8. (Previously Presented) The apparatus as recited in claim 1, wherein said single, atomic cryptographic instruction implicitly references a plurality of registers within said x86-compatible microprocessor.

9. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said ~~one of the cryptographic operations~~encryption operation is to be accomplished.

10. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of ~~a correspondingsaid~~ corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said ~~one of the cryptographic operations upon a~~encryption operation upon said plurality of input text blocks.

11. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within ~~a pluralitysaid~~ plurality of input text blocks.

12. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said ~~one of the cryptographic operations~~encryption operation.

13. (Original) The apparatus as recited in claim 12, wherein said user-generated key schedule comprises said cryptographic key data.

14. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said ~~one of the cryptographic operations~~encryption operation.

15. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said ~~one of the cryptographic operations~~encryption operation, wherein said control word prescribes cryptographic parameters for said encryption operation, and wherein said control word comprises:

a keygen field, configured to specify that said user-generated key schedule be employed during execution of said encryption operation.

16. (Cancelled)

17. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a cryptography unit within an x86-compatible microprocessor, configured to execute one of the cryptographic operations responsive to receipt of a single, atomic cryptographic instruction within an application program that prescribes a decryption operation, ~~wherein said single, atomic cryptographic instruction is arranged according to the instruction format for execution on said x86-compatible microprocessor, and wherein said x86-compatible microprocessor executes said application program, and~~ wherein said single, atomic cryptographic instruction also prescribes that a user-generated key schedule be employed when executing said decryption operation, and wherein said decryption operation that is prescribed by said single, atomic cryptographic instruction comprises decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks, and wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction;

an x86 integer unit, an x86 floating point unit, an x86 MMX unit, and an x86 SSE unit, each of said units also disposed within said x86-compatible microprocessor, wherein said cryptography unit operates in parallel with said x86 integer unit, said x86 floating point unit, said x86 MMX unit, and said x86 SSE unit, to accomplish said decryption operation, wherein said x86 integer unit executes a second plurality of micro instructions generated by said translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said plurality of cryptographic rounds; and

a keygen unit, operatively coupled to said cryptography unit, configured to direct said x86-compatible microprocessor to perform said ~~one of the cryptographic~~decryption operation ~~operations~~ and to employ said user-generated key schedule when performing said decryption operation.

18. (Original) The apparatus as recited in claim 17, wherein said user-generated key schedule is stored in memory.

19. (Original) The apparatus as recited in claim 17, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

20. (Previously Presented) The apparatus as recited in claim 17, wherein said keygen unit is configured to interpret a key generation field within a control word which is referenced by said single, atomic cryptographic instruction.

21. (Cancelled)

22. (Currently Amended) A method for performing cryptographic operations in a x86-compatible microprocessor, the method comprising:

executing an application program that is stored in memory, said executing comprising:

receiving a single, atomic cryptographic instruction from the memory that prescribes employment of a user-generated key schedule during execution of an encryption operation, ~~wherein the single, atomic cryptographic instruction is one of the instructions in the application program, wherein the single, atomic cryptographic instruction is arranged according to the instruction format for execution on the x86-compatible microprocessor, and~~ wherein the encryption operation that is executed responsive to the single, atomic cryptographic instruction comprises execution of a plurality of cryptographic rounds on ~~encryption of~~ a plurality of plaintext blocks to generate a corresponding plurality of ciphertext ~~blocks; and~~blocks;

within a cryptographic unit in the x86-compatible microprocessor, employing the user-generated key schedule when executing the encryption operation to generate a result of the encryption operation, wherein the cryptographic unit executes a first plurality of micro instructions generated by translation of the single, atomic cryptographic instruction; and

within an integer unit in the x86-compatible microprocessor, executing a second plurality of micro instructions generated by the translation to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of the plurality of cryptographic rounds.

23. (Previously Presented) The method as recited in claim 22, wherein said receiving comprises:

via a field within a control word that is referenced by the single, atomic cryptographic instruction, specifying employment of the user-generated key schedule.

24. (Original) The method as recited in claim 22, wherein said employing comprises:

loading the user-generated key schedule from memory.

25. (Original) The method as recited in claim 22, wherein the user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm.

26. (Cancelled)